Microsoft SSE Deep Dive

- Thomas Detzner

- Microsoft

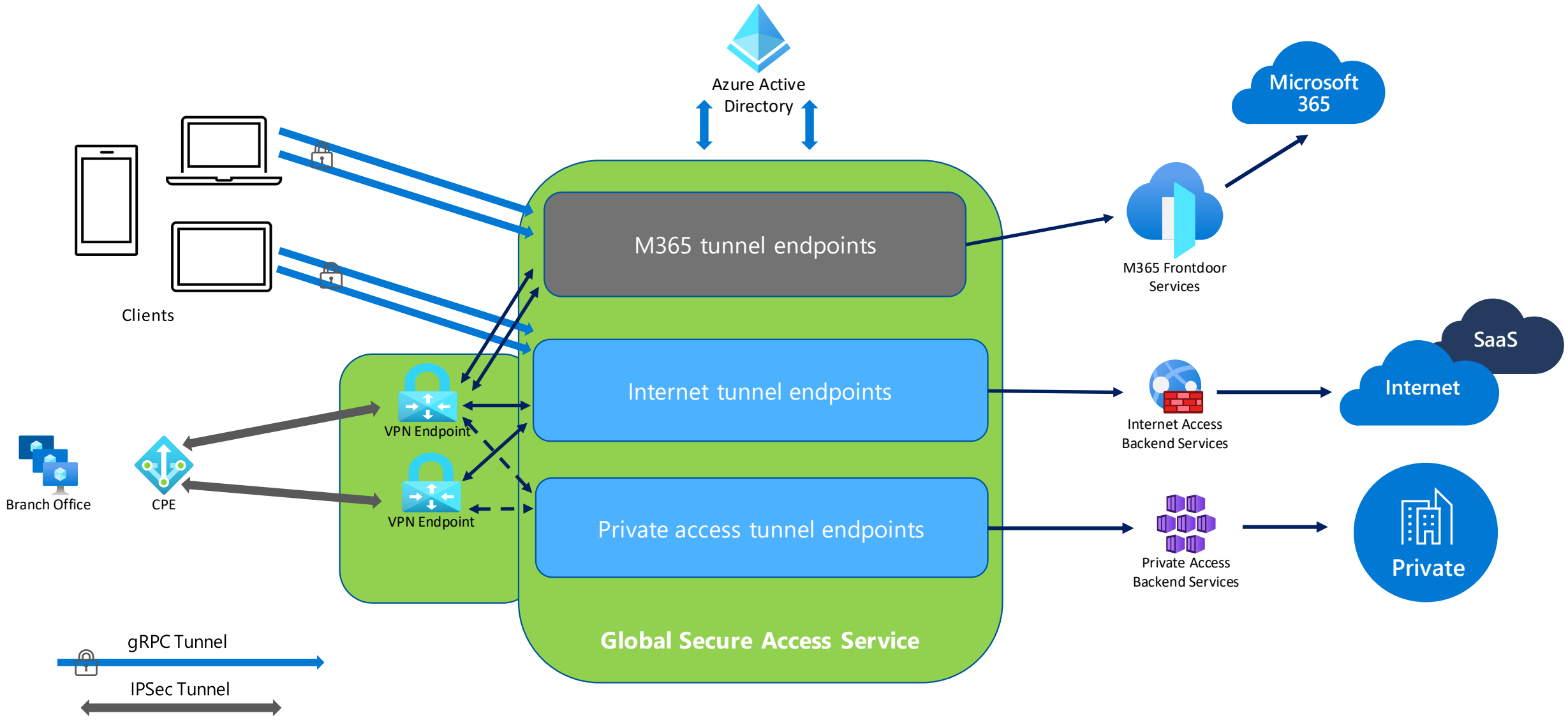
- December 2023

Agenda

- High Level Service Architecture
- Client Architecture Details
  - Tunnel details
- Traffic Acquisition
  - Basics
  - Policy Details
- Troubleshooting Deep Dives
  - Client checker
  - Health check tool
  - Wireshark

High Level Service Architecture

Microsoft SSE High Level Architecture



Protocol fundamentals

What is gRPC?

- gRPC: (google) RPC - Remote Procedure Calls
- RPCs are a form of inter-process communication (IPC), in that different processes have different address spaces
- High-performance, general-purpose RPC framework https://grpc.io/
- Much more network efficient then REST API calls on the wire
- Part of Cloud Native Computing Foundation as incubation project
- Multi-platform, multi-language framework
- Used by Google, Square, Netflix and others

CLOUD NATIVE
COMPUTING FOUNDATION

What is gRPC?

- Extensibility points for custom implementations
- Support for 10+ programming languages
- Bi-directional streaming and integrated authentication
- Allows for simple service definition and extensibility

ProtoBuf

```
syntax = "proto3";

service Greeter {
  rpc SayHello (HelloRequest) returns (HelloReply);
}

message HelloRequest {
  string name = 1;
}

message HelloReply {
  string message = 1;
}
```

C#

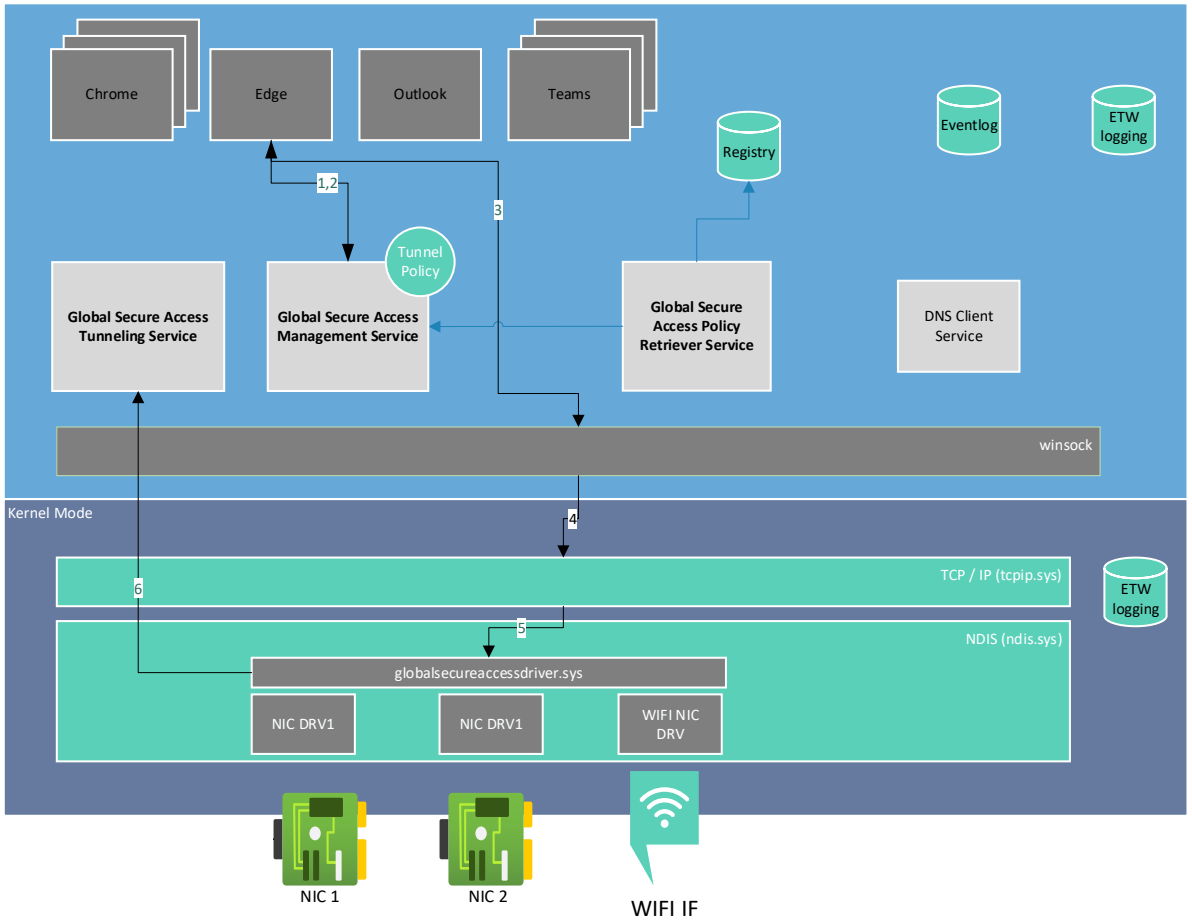
```
public class GreeterService : Greeter.GreeterBase
{
    private readonly ILogger<GreeterService> _logger;
    public GreeterService(ILogger<GreeterService> logger)
    {
        _logger = logger;
    }

    public override Task<HelloReply> SayHello(HelloRequest request, ServerCallContext context)
    {
        return Task.FromResult(new HelloReply
        {
            Message = "Hello " + request.Name
        });
    }
}
```

```
20  require dirname(__FILE__) . '/vendor/autoload.php';
21
22  class Greeter extends Helloworld\GreeterStub
23  {
24      public function SayHello(
25          \Helloworld\HelloRequest $request,
26          \Grpc\ServerContext $serverContext
27      ): ?\Helloworld\HelloReply {
28          $name = $request->getName();
29          echo 'Received request: ' . $name . PHP_EOL;
30          $response = new \Helloworld\HelloReply();
31          $response->setMessage("Hello " . $name);
32          return $response;
33      }
34  }
35
36  $port = 50051;
37  $server = new \Grpc\RpcServer();
38  $server->addHttp2Port('0.0.0.0:'.$port);
39  $server->handle(new Greeter());
40  echo 'Listening on port :' . $port . PHP_EOL;
41  $server->run();
```

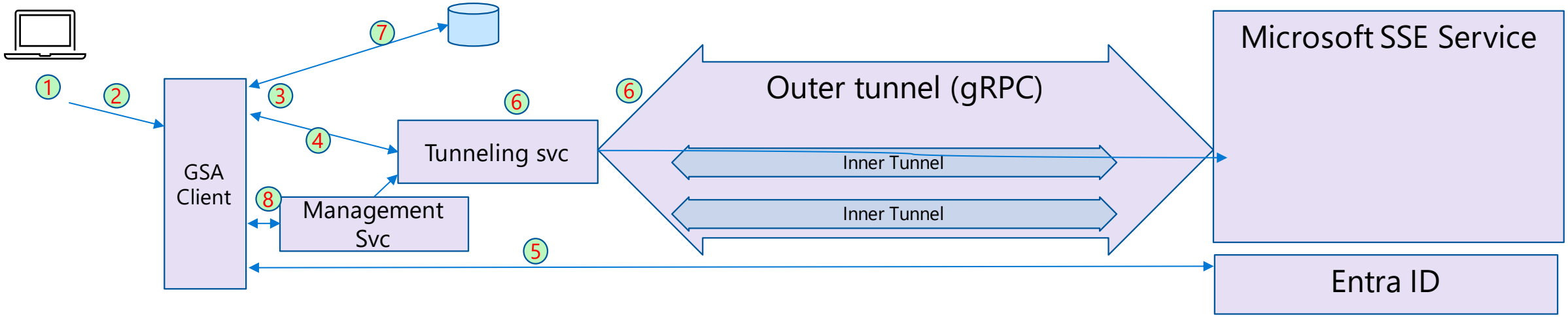
Client Details

Global Secure Access Client Architecture | Windows

- Client agent using Kernel Mode and User Mode components
- Configuration policy agent to retrieve tenant specific configuration
- Traffic acquisition and encryption handling
- Using gRPC to communicate to the cloud service



Client Details | Tunnel Authentication



1. Device is trying to communicate with an internet resource.
2. The client agent intercepts the first IP packet and determines the packet is to be acquired.
3. The client agent checks if any outer tunnel instance is present. If not, reaches out to Tunneling client to create the outer tunnel instance.
4. The Global Secure Access service forces Entra ID user authentication to create an authenticated Tunnel.
5. The client initiates an Entra ID AuthN and provides the access token to the client, client stores it locally.
6. A new inner Tunnel is created with additional connection details and send to the Global Secure Access service, which validates and creates an authenticated Tunnel (inner tunnel) instance.
7. The client agent stores tunnel instance information.
8. The client decides to send traffic to the Global Secure Access service with a specific Channel identifier.

Traffic Acquisition

Traffic Acquisition | Basics

Starting point is the portal

Traffic forwarding

Refresh | Got feedback?

Manage traffic forwarding profiles

Traffic forwarding profiles enabled admins to select which traffic should be acquir
Once selected, the forwarding profiles are assigned to any device in the tenant th
The ability to assign forwarding profiles to users and groups will be added in the f

Traffic forwarding profiles for Microsoft 365 and Internet can be assigned to remo
client less devices. Learn more

Microsoft 365 profile	Private acces
Enabled	Disabled
Last modified on 07/13/2023, 05:59 PM	Last modified on
Applies to All Microsoft 365 traffic	Applies to Private resources
Microsoft 365 traffic policies 3 policies View	Private access p Quick Access, 0 A
Linked Conditional Access policies 1 policy View	Linked Conditic None
Assignments All client devices 0 assigned remote networks	Assignments All client devices
Add assignments	Add assignm

Policies & rules (Microsoft 365 profile)

Traffic Profile

Global Secure Access only acquires TCP traffic (HTTP/HTTPS). Branches acquire IP-identifiable traffic.

Please note that we are working on acquiring additional Microsoft 365 traffic. Complete Office 365 URLs and IP address ranges can be found here. Office 365 URLs and IP address ranges

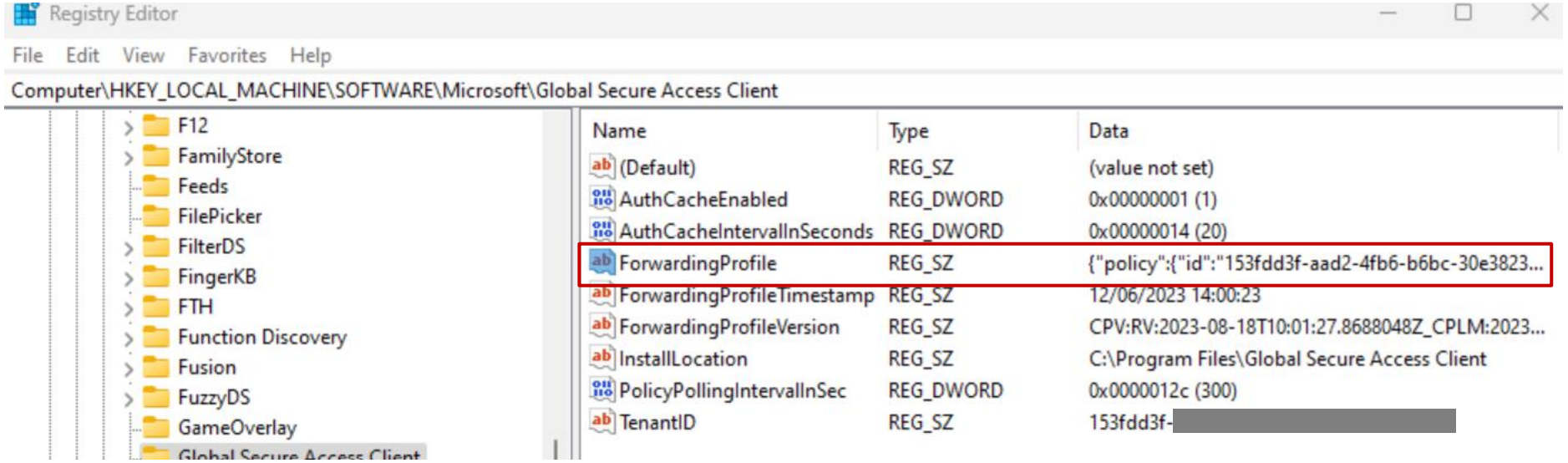
Policy	Enable/Disable	Destinati...	Destination	Ports	Category	Protoc...	Action
Exchange Online	✓						
Rules							
		Fqdn	outlook.office.com, outlook.office36!	80, 443	Optimized	Tcp	Forward
		IpSubnet	13.107.6.152/31, 13.107.18.10/31, 13	80, 443	Optimized	Tcp	Forward
		Fqdn	*.outlook.com	80, 443	Default	Tcp	Forward
		Fqdn	*.protection.outlook.com	443	Allow	Tcp	Forward
		IpSubnet	40.92.0.0/15, 40.107.0.0/16, 52.100.0	443	Allow	Tcp	Forward
		Fqdn	autodiscover.*.onmicrosoft.com	80, 443	Default	Tcp	Forward
SharePoint Online and OneDrive for Business	✓						
Rules							
		Fqdn	*.sharepoint.com	80, 443	Optimized	Tcp	Forward
		IpSubnet	13.107.136.0/22, 40.108.128.0/17, 52	80, 443	Optimized	Tcp	Forward
		Fqdn	ssw.live.com, storage.live.com	443	Default	Tcp	Forward
		Fqdn	*.search.production.apac.trafficmana	443	Default	Tcp	Forward
		Fqdn	*.wns.windows.com, admin.onedrive.	80, 443	Default	Tcp	Forward
		Fqdn	g.live.com, oneclient.sfx.ms	80, 443	Default	Tcp	Forward
		Fqdn	*.sharepointonline.com, spoprod-a.a	80, 443	Default	Tcp	Forward
		Fqdn	*.svc.ms	80, 443	Default	Tcp	Forward
Microsoft 365 Common and Office Online	✓						

Traffic Acquisition | Basics

The Global Secure Access Policy Retriever Service talks to the Microsoft SSE Service to retrieve the policy

Writes the Policy to the local registry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Global Secure Access Client`



Traffic Acquisition | Basics

The policy (Regvalue in **`ForwardingProfile`**) is a json object

Use your favorite json converter to show (copy&paste)

E.g. VS Code

CurrentPolicytdetzner.json

CurrentPolicytdetzner.json > {} policy > [ ] channels > {} 0 > name


```
{
    "configuration": {
        "apsSettings": {
            "requestPollingIntervalInSeconds": 300
        },
        "edsSettings": {
            "pollingIntervalInSeconds": 10
        },
        "flowHandler": {
            "graceTimeInMs": 3500
        },
        "managementService": {
            "authenticationCacheRefreshIntervalInSeconds": 20,
            "cacheAuthenticationToken": true,
            "hostAcquisitionInternalSubNet": {
                "subnetAddress": 101056512,
                "subnetMask": 4294901760
            },
            "policyUpdateFlushOsCache": false
        },
        "userModeLogs": {
            "directoryPath": "c:\naaslogs",
            "fileCount": 3,
            "logSizeInMB": 2.0
        }
    },
    "controlPlanePoliciesVersion": "20230706130454.000",
    "policy": {
        "channels": [
            {
                "diagnosticUri": "https://m365.edgediagnostic.globalsecureaccess.microsoft.com:6543/connectivitytest/ping",
                "edgesSettings": {
                    "primaryEdges": [
                        {
                            "edgeAddress": "135a0f48-eb72-4859-8509-0ef1a2791f1a.m365.client.globalsecureaccess.microsoft.com",
                            "edgePort": 443,
                            "isSecure": true
                        }
                    ],
                    "secondaryEdges": []
                },
                "id": "98443393-7d7f-436d-a01a-6a8f11ab3e34",
                "naasAuthorizationTokenContext": {
                    "audienceScope": "128b0dd9-1511-459e-9f95-168f2376341c/NetworkProfile.M365",
                    "clientAppId": "d5e23a82-d7e1-4886-af25-27037a0fdc2a",
                    "clientRedirectUri": "https://login.microsoftonline.com/common/oauth2/nativeclient"
                },
                "name": "M365"
            }
```

Traffic Acquisition | Basics | Graph API

The forwarding policy can be accessed/created via API as well

Secure access to cloud, public, and private apps using Microsoft Graph network access APIs - Microsoft Graph beta | Microsoft Learn

Examples:

List forwardingPolicies - Microsoft Graph beta | Microsoft Learn

```
GET https://graph.microsoft.com/beta/networkAccess/{forwardingProfileId}/forwardingPolicies
```

GET https://graph.microsoft.com/beta/networkaccess/forwardingProfiles

Get the rules:

GET https://graph.microsoft.com/beta/networkaccess/forwardingPolicy/{forwardingPolicyId}/policyRules/

Policy Details

Traffic Acquisition | Policy | Channels – InternetM365


```
"policy": {
        "channels": [
            {
                "diagnosticUri": "https://m365.edgediagnostic.globalsecureaccess.microsoft.com:6543/connectivitytest/ping",
                "edgesSettings": {
                    "primaryEdges": [
                        {
                            "edgeAddress": "135a0f48-eb72-4859-8509-0ef1a2791f1a.m365.client.globalsecureaccess.microsoft.com",
                            "edgePort": 443,
                            "isSecure": true
                        }
                    ],
                    "secondaryEdges": []},
                "id": "",
                "naasAuthorizationTokenContext": {98443393-7d7f-436d-a01a-6a8f11ab3e34
                    "audienceScope": "128b0dd9-1511-459e-9f95-168f2376341c/NetworkProfile.M365",
                    "clientAppId": "d5e23a82-d7e1-4886-af25-27037a0fdc2a",
                    "clientRedirectUri": "https://login.microsoftonline.com/common/oauth2/nativeclient"
                },
                "name": "M365"
            },
```

Traffic Acquisition | Policy | Channels - PrivateAccess


```
"policy": {
        {
                "diagnosticUri": "https://private.edgediagnostic.globalsecureaccess.microsoft.com/connectivitytest/ping",
                "edgesSettings": {
                    "primaryEdges": [
                        {
                            "edgeAddress": "135a0f48-eb72-4859-8509-0ef1a2791f1a.private.client.globalsecureaccess.microsoft.com",
                            "edgePort": 443,
                            "isSecure": true
                        }
                    ],
                    "secondaryEdges": []
                },
                "id": "f3ceb6cc-1706-4817-a2d7-2a8ff07f474c",
                "naasAuthorizationTokenContext": {
                    "audienceScope": "128b0dd9-1511-459e-9f95-168f2376341c/NetworkProfile.Private",
                    "clientAppId": "760282b4-0cfc-4952-b467-c8e0298fee16",
                    "clientRedirectUri": "https://login.microsoftonline.com/common/oauth2/nativeclient"
                },
                "name": "Private"
            }
```

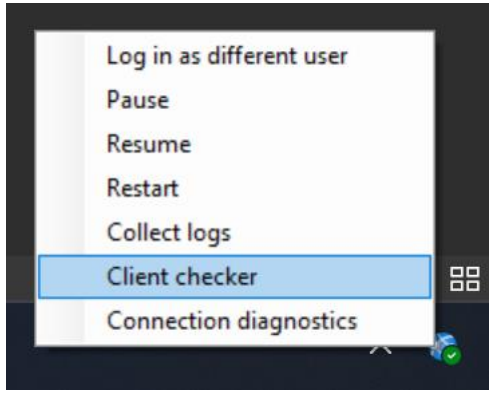
Traffic Acquisition | Policy | Demo

Troubleshooting Deep Dives | Examples and Demo

Troubleshooting Deep Dives | Client checker tool

Start with the Client Checker tool

Investigate all failed issues



C:\Program Files\Global Secure Access Client\GlobalSecureAccessClientChecker.exe

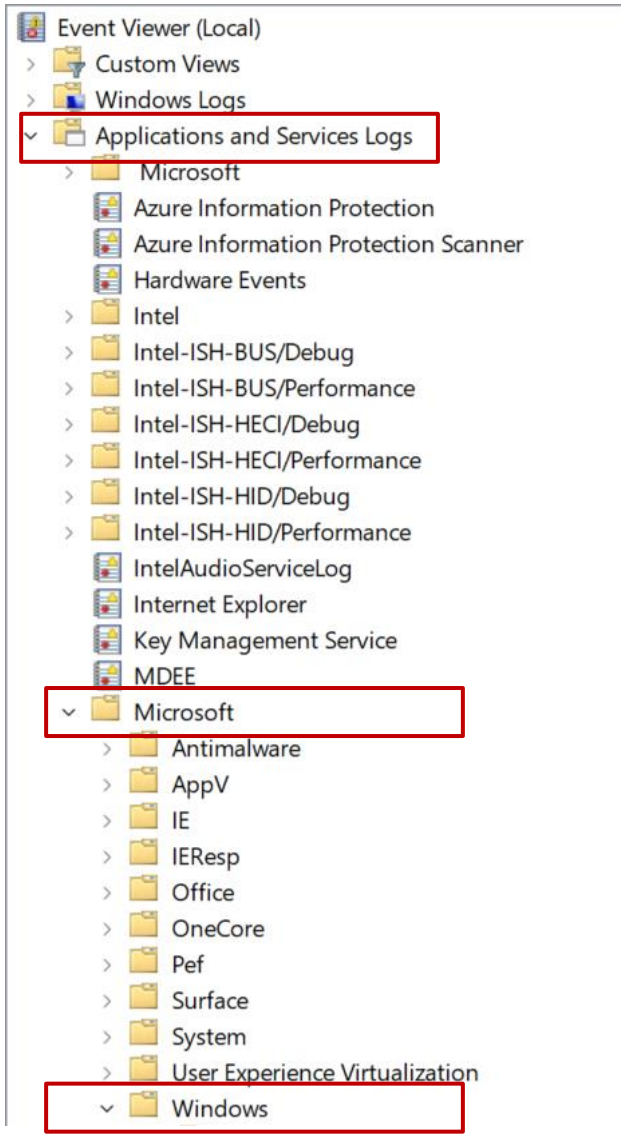
```
Starting Client Checker tool
Is device AAD joined: YES
Process GlobalSecureAccessTunnelingService is running: YES
Process GlobalSecureAccessManagementService is running: YES
Process GlobalSecureAccessPolicyRetrieverService is running: YES
Process GlobalSecureAccessClient is running: YES
GlobalSecureAccessDriver is running: YES
Forwarding profile Registry exists: YES
The forwarding profile matches the expected schema: YES
Breakglass mode disabled: YES
Channel M365 diagnosticUri in policy: YES
Channel Private diagnosticUri in policy: YES
Is secure DNS disabled in OS?: YES
Is secure DNS disabled in Edge?: YES
DNS responsive: YES
Magic IP received for FQDN m365.edgediagnostic.globalsecureaccess.microsoft.com: YES
Is IPv4 preferred: NO
Cached token: YES
M365's edge reachable: YES
Private's edge reachable: YES
Manual proxy is disabled: YES
M365 tunneling success: YES
Private tunneling success: YES
Global Secure Access processes are healthy and not crashing in the last 24h: YES
Other processes are healthy and not crashing in the last 24h: YES
Is QUIC disabled in Edge?: YES
No Windows Firewall rules related to QUIC found
Finished Client Checker tool, press any key to exit
```

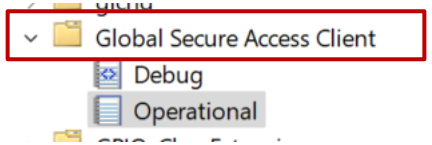
Troubleshooting Deep Dives | Eventlog

- The client has rich Event log support
- Lives under the Application and Services logs

- Operational Log:
  - Connection handling and errors
  - Authentication handling and errors

- Debug Log:
  - Detailed traffic flow handling
  - Traffic that is acquired and not acquired





Troubleshooting Deep Dives | Eventlog

Information	23.07.2023 21:39:10	Microsoft-Global Secure Access Clien
Information	23.07.2023 21:39:05	Microsoft-Global Secure Access Clien

Event 142, Microsoft-Global Secure Access Client

General Details

Connection to Global Secure Access edge succeeded (GRPC connection established) - Channel f3ceb6cc-1706-4817-a2d7-2a8ff07f474c, Destination IP/Port 135a0f48-eb72-4859-8509-0ef1a2791f1a.private.client.globalsecureaccess.microsoft.com/443, Is Secure: true, Channel State: GRPC_CHANNEL_READY

Information	23.07.2023 21:38:56	Microsoft-Global Secure Access Clien

Event 221, Microsoft-Global Secure Access Client

General Details

A change in the forwarding profile was detected. Loading the new forwarding profile. Previous Version: , Current Version: CPV:RV:2023-07-17T01:19:47.8729543Z_CPLM:20230706130454.000_NAV:TenantSpecificVersion_12

Troubleshooting Deep Dives | Connection Diagnostics

Super useful tool to understand traffic handling

Leverage Flows and Hostname acquisition tabs:

Global Secure Access Client Connection Diagnostics

File

Summary | Flows | Hostname Acquisition | Services | Channels

TimeStamp	FQDN	Source Port	Destination IP	Destination Port	Protocol	Process Name	State	Sent Data[Bytes]	Received Data[Bytes]	Auth Time	Correlation ID	Flow ID	Channel Name	Tunnel ID
7/19/2023 3:32:22 PM	private.edgediagnostic.globalsecureaccess.microsoft.com	63794	6.6.0.14	443	Tcp	GlobalSecureAccessClient.exe	Closed	1147	1490	324,0272 ms	JaTXpa/zj0WOsYMj.0.0	228516	Private	0
7/19/2023 3:32:23 PM	m365.edgediagnostic.globalsecureaccess.microsoft.com	63795	6.6.0.15	6543	Tcp	GlobalSecureAccessClient.exe	Closed	1163	1307	696,5476 ms	SumvvKHOAkiw7OlO.0.0	228517	M365	1
7/19/2023 3:32:24 PM	N/A	63796	20.190.190.103	443	Tcp	Teams.exe	Closed	5282	7306	1,1241 ms	/3PlwDMdckCQ6EIQ.0.0	228520	M365	1
7/19/2023 3:32:25 PM	N/A	63797	13.107.136.8	443	Tcp	Teams.exe	Closed	5745	79455	0,7056 ms	WUhG5g3NvUmuTLFO.0.0	228523	M365	1
7/19/2023 3:32:25 PM	westeurope1-mediap.svc.ms	63798	6.6.0.23	443	Tcp	Teams.exe	Closed	3404	78914	0,7678 ms	WzudXHG+lE+EPoDq.0.0	228525	M365	1
7/19/2023 3:32:27 PM	N/A	63799	40.99.157.50	443	Tcp	OUTLOOK.EXE	Closed	2901	368	0,5771 ms	kwsaNOc/+0WSE9aA.0.0	228537	M365	1
7/19/2023 3:32:27 PM	N/A	63800	40.99.157.50	443	Tcp	OUTLOOK.EXE	Closed	2912	368	0,5465 ms	KAU8AEuQJUeyPy0d.0.0	228538	M365	1
7/19/2023 3:32:27 PM	N/A	63801	40.99.157.50	443	Tcp	OUTLOOK.EXE	Closed	3078	2071	0,6487 ms	iVIFUV8RbUy6bc4x.0.0	228539	M365	1
7/19/2023 3:32:32 PM	m365.edgediagnostic.globalsecureaccess.microsoft.com	63803	6.6.0.15	6543	Tcp	GlobalSecureAccessClient.exe	Closed	1203	1307	0,6622 ms	MsV6A9Tz+0yOZKn1.0.0	228553	M365	1

Global Secure Access Client Connection Diagnostics

File

Summary | Flows | Hostname Acquisition | Services | Channels

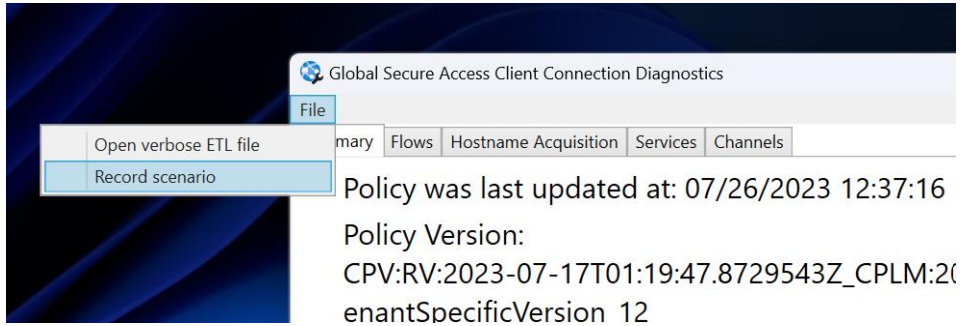
TimeStamp	FQDN	Generated IP Address	Original IPv4 Address	Handling Time	Packet ID
7/19/2023 3:44:45 PM	officeclient.microsoft.com	6.6.0.17	52.109.32.24	1,7946 ms	100204
7/19/2023 3:40:18 PM	client.wns.windows.com	6.6.0.24	40.115.3.253	1,5804 ms	99930
7/19/2023 3:34:55 PM	officeclient.microsoft.com	6.6.0.17	52.109.28.100	8,588 ms	99536
7/19/2023 3:32:52 PM	m365.edgediagnostic.globalsecureaccess.microsoft.com	6.6.0.15	0.0.0.0	2,0281 ms	99378
7/19/2023 3:32:52 PM	private.edgediagnostic.globalsecureaccess.microsoft.com	6.6.0.14	0.0.0.0	1,8656 ms	99377
7/19/2023 3:32:25 PM	westeurope1-mediap.svc.ms	6.6.0.23	13.107.136.13	2,4708 ms	99351

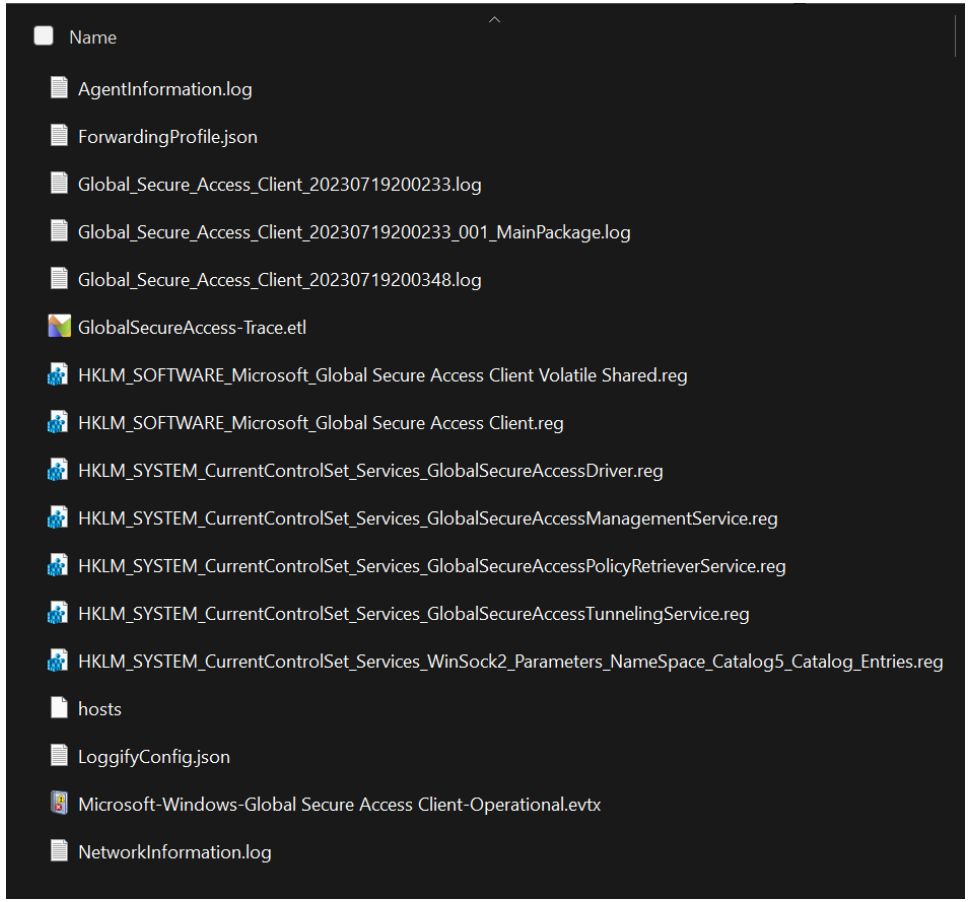
Troubleshooting Deep Dives | collect logs

In case of issues with the client / traffic handling, you may need client side data, Two main ways:

1. Using the tray option " Collect Logs"

2. Using the option "Record Scenario"





3. Logs will be created in `C:\Program Files\Global Secure Access Client\Logs`

Troubleshooting Deep Dives | Wireshark

If all of the before did not help and you collected logs

Open the NetworkTrace.pcap in wireshark

If the Tunnels do not come up, start with the endpoints from the policy config:

```
"edgeAddress": "135a0f48-eb72-4859-8509-0ef1a2791f1a.m365.client.globalsecureaccess.microsoft.com",
```

C:\Windows\system32\cmd.exe

```
C:\Users\JohnDoe>nslookup 153fdd3f-aad2-4fb6-b6bc-30e3823ea51b.m365.client.globalsecureaccess.microsoft.com
Server:  fritz.box
Address:  192.168.188.11

Non-authoritative answer:
Name:    ztna1p-0001.ztna1p-msedge.net
Address:  13.107.232.10
Aliases:  153fdd3f-aad2-4fb6-b6bc-30e3823ea51b.m365.client.globalsecureaccess.microsoft.com
          ztna1p-ring.msedge.net
          ztna1p-ring.ztna1p-0001.ztna1p-msedge.net
```

Troubleshooting Deep Dives | Wireshark

If all o

logs

Open

If the

endp

"edgeA
0ef1a2
com",

C:\Win

C:\Users
Server:
Address:

Non-auth
Name:
Address:
Aliases:

NetworkTrace.pcap

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

ip.addr==13.107.232.10 || ip.addr==150.171.15.10

No.	Time	Source	Destination	Protocol	Length	Info
1661…	0.001517	10.174.85.251	13.107.232.10	TCP	66	61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SACK_PERM
1661…	0.000003	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000004	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000001	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000002	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000002	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000001	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000001	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000002	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000000	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000003	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1661…	0.000002	10.174.85.251	13.107.232.10	TCP	66	[TCP Retransmission] 61688 → 443 [SYN] Seq=0 Win=64202 Len=0 MSS=1366 WS=256 SA
1662…	0.000198	13.107.232.10	10.174.85.251	TCP	66	443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1366 SACK_PERM WS=1024
1662…	0.000002	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000002	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000001	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000002	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000001	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000000	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000001	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000002	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000002	13.107.232.10	10.174.85.251	TCP	66	[TCP Retransmission] 443 → 61688 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=136
1662…	0.000178	10.174.85.251	13.107.232.10	TCP	54	61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000001	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#1] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000004	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#2] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000001	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#3] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000002	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#4] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000003	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#5] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000001	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#6] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000001	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#7] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000002	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#8] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000001	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#9] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
1662…	0.000003	10.174.85.251	13.107.232.10	TCP	54	[TCP Dup ACK 166256#10] 61688 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0

Troubleshooting Deep Dives | Wireshark

For looking inside the tunnel, filter on the synthetic IP addresses:

Global Secure Access Client ETL viewer - C:\temp\GlobalSecureAccess-Trace.etl

Flows | Host Name Acquisition

TimeStamp	FQDN	Source Port	Destination IP	Destination Port	Protocol	Process Name	State	Sent Data[Bytes]	Received Dat
12/6/2023 2:26:09 PM	client.wns.windows.com	49734	6.6.0.2	443	Tcp	svchost.exe	Active	0	0
12/6/2023 2:26:09 PM	login.microsoftonline.com	49738	6.6.0.1	443	Tcp	backgroundTaskHost.exe	Closed	6066	1363
12/6/2023 2:26:09 PM	outlook.office365.com	49742	6.6.0.3	443	Tcp	StartMenuExperienceHost.exe	Closed	1448	6987
12/6/2023 2:26:09 PM	officeclient.microsoft.com	49743	6.6.0.4	443	Tcp	StartMenuExperienceHost.exe	Closed	1410	7880

NetworkTrace.pcap

Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

ip.addr == 6.6.0.3

No.	Time	Source	Destination	Protocol	Length	Info
85…	0.00…	192.168.188.54	6.6.0.3	TCP	66	49903 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
85…	0.00…	192.168.188.54	6.6.0.3	TCP	66	[TCP Retransmission] 49903 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
88…	0.00…	6.6.0.3	192.168.188.54	TCP	66	443 → 49903 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 SACK_PE
88…	0.00…	6.6.0.3	192.168.188.54	TCP	66	[TCP Retransmission] 443 → 49903 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
89…	0.00…	6.6.0.3	192.168.188.54	TCP	66	[TCP Retransmission] 443 → 49903 [SYN, ACK] Seq=0 Ack=1 Win=65535 Le
89…	0.00…	192.168.188.54	6.6.0.3	TCP	54	49903 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
89…	0.00…	192.168.188.54	6.6.0.3	TCP	54	[TCP Dup ACK 8907#1] 49903 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
89…	0.00…	6.6.0.3	192.168.188.54	TCP	66	[TCP Out-Of-Order] 443 → 49903 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
91…	0.00…	192.168.188.54	6.6.0.3	TLS…	627	Client Hello (SNI=outlook.office365.com)
91…	0.00…	192.168.188.54	6.6.0.3	TCP	627	[TCP Retransmission] 49903 → 443 [PSH, ACK] Seq=1 Ack=1 Win=262656 L
93…	0.00…	6.6.0.3	192.168.188.54	TCP	54	443 → 49903 [ACK] Seq=1 Ack=574 Win=67584 Len=0
93…	0.00…	6.6.0.3	192.168.188.54	TCP	54	[TCP Dup ACK 9396#1] 443 → 49903 [ACK] Seq=1 Ack=574 Win=67584 Len=0
93…	0.00…	6.6.0.3	192.168.188.54	TCP	54	[TCP Dup ACK 9396#2] 443 → 49903 [ACK] Seq=1 Ack=574 Win=67584 Len=0
93…	0.00…	6.6.0.3	192.168.188.54	TCP	54	[TCP Dup ACK 9396#3] 443 → 49903 [ACK] Seq=1 Ack=574 Win=67584 Len=0
94…	0.00…	6.6.0.3	192.168.188.54	TLS…	153	Hello Retry Request, Change Cipher Spec
94…	0.00…	6.6.0.3	192.168.188.54	TCP	153	[TCP Retransmission] 443 → 49903 [PSH, ACK] Seq=1 Ack=574 Win=67584
94…	0.00…	6.6.0.3	192.168.188.54	TCP	153	[TCP Retransmission] 443 → 49903 [PSH, ACK] Seq=1 Ack=574 Win=67584

In closing …

Call to Action

1. Start with Global Secure Access today, latest tomorrow
2. Enable the M365 Traffic profile and assign a CA policy
    1. If you have on-premises or IaaS test servers, start with Private access as well
3. Identify a few test clients, install the Global Secure Access Client
4. Get your hands dirty
5. Let us know if you have any feedback, want to learn more!

One more thing …

Global Secure Access Client - Advanced diagnostics

Overview | Health check | Forwarding profile | Hostname acquisition | Traffic

Connection to one or more of the diagnostic URLs failed

Health check

These checks verify the health of the Global Secure Access client. Learn more

Refresh

Device is Microsoft Entra joined	Yes
Tunneling service running	Yes
Management service running	Yes
Policy Retriever service running	Yes
Driver running	Yes
Client tray application running	Yes
Forwarding profile registry exists	Yes
Forwarding profile matches expected schema	Yes
Breakglass mode disabled	Yes
Diagnostic URLs in forwarding profile	Yes
Secure DNS disabled in OS	Yes
Secure DNS disabled in browsers (Edge, Chrome, Firefox)	Yes
DNS responsive	Yes
Magic IP received	Yes
IPV4 preferred	Yes
Cached token	Yes
Edges are reachable	Yes
Proxy disabled	Yes
Tunneling succeeded	No
Global Secure Access processes healthy (last 24h)	Yes

Global Secure Access Client - Advanced diagnostics

Overview | Health check | Forwarding profile | Hostname acquisition | Traffic

Forwarding profile details

View all the rules applied to this client. Learn more

Forwarding profile ID	CPV:RV:2023-12-05T06:08:19.7790242Z_CPLM:20231205060555.000_NAV:TenantSpecificVersion_13
Forwarding profile last updated	06.12.2023 15:43:36

Refresh details

Rules

Add filter | Columns

Microsoft 365 rules

Presentation last saved: Just now

Private access rules

Priority	Destination (IP/FQDN)	Protocol	Port	Action
2	private.edgediagnostic.globalsecure...	TCP	0 - 65535	Tunnel

Internet access rules

Priority	Destination (IP/FQDN)	Protocol	Port	Action
3	internet.edgediagnostic.globalsecur...	TCP	0 - 65535	Tunnel
103	msedge.net	TCP	443, 80, 8080	Bypass
103	*.msftvpn-alt.ras.microsoft.com	TCP	443, 80, 8080	Bypass
103	msftvpn.ras.microsoft.com	TCP	443, 80, 8080	Bypass
103	msftvpn-alt.ras.microsoft.com	TCP	443, 80, 8080	Bypass
103	*.vpn.azure.com	TCP	443, 80, 8080	Bypass
103	*.msftvpn.ras.microsoft.com	TCP	443, 80, 8080	Bypass
103	c-msedge.net	TCP	443, 80, 8080	Bypass
103	www.msftconnecttest.com	TCP	443, 80, 8080	Bypass
103	www.msftncsi.com	TCP	443, 80, 8080	Bypass

Global Secure Access Client - Advanced diagnostics

Overview | Health check | Forwarding profile | Hostname acquisition | Traffic

Network traffic

Collect and analyze this device's network traffic. Learn more

Stop collecting | Export CSV | Clear table | Add filter | Columns

Process name != GlobalSecureAccessClient.exe | Action == Tunnel

Collecting network and DNS traffic

Timestamp begin	Connection status	Protocol	Destination FQDN	Destination IP	Destination port	Correlation vector ID	Process name
06.12.2023 15:45:10	Closed	TCP	login.microsoftonline.com	6.6.3.141	443	iyJHvUmoekOhCJae.0.0	backgroundTaskHost.ex
06.12.2023 15:45:16	Active	TCP	www.actionablemessage.olk	6.6.4.147	80	33Z1/NMVvUyvJ/Kg.0.0	msedgewebview2.exe
06.12.2023 15:45:17	Closed	TCP	login.microsoftonline.com	6.6.3.141	443	lOldg6e7dEm0JXg3.0.0	backgroundTaskHost.ex
06.12.2023 15:45:18	Active	TCP	82492-ipv4v6.gr.global.aa-rt.sharepoint.com	6.6.4.71	443	Xr/Z9KlccEmZcrJf.0.0	OneDrive.exe
06.12.2023 15:45:26	Active	TCP	azwu3cmg.westus2.cloudapp.azure.com	6.6.4.246	443	qdHl70A5i0eB/XUU.0.0	CcmExec.exe
06.12.2023 15:45:31	Active	TCP	js.monitor.azure.com	6.6.4.125	443	u+CwWcwQXk+VcoV+.0.0	msedge.exe
06.12.2023 15:45:31	Active	TCP	mscom.demdex.net	6.6.4.126	443	VpCqEhoGXk+Yjt2i.0.0	msedge.exe
06.12.2023 15:45:31	Active	TCP	mdec.nelreports.net	6.6.6.200	443	w62ImwttX069iM5c.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	browser.events.data.msn.com	6.6.4.70	443	7BYdA7y+AUaB2BXu.0.0	msedge.exe
06.12.2023 15:45:34	Closed	TCP	browser.events.data.msn.com	6.6.4.70	443	tU7l09HSqEeFbikV.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	r.msftstatic.com	6.6.4.254	443	JUgDLzVFtUaWj0IG.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	r.bing.com	6.6.4.103	443	drBSBJJWTkun2J8m.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	r.msftstatic.com	6.6.4.254	443	VLxItjENVkmI69uH.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	r.bing.com	6.6.4.103	443	QorqCaijyEm4ccHY.0.0	msedge.exe
06.12.2023 15:45:34	Closed	TCP	browser.events.data.msn.com	6.6.4.70	443	ghOsI3b1A0WUZ5tb.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	c.msn.com	6.6.4.253	443	c/w1bMc7bUmFFLRI.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	graph.microsoft.com	6.6.4.89	443	gyIlKNhJhUmdbsg5.0.0	msedge.exe
06.12.2023 15:45:34	Active	TCP	graph.microsoft.com	6.6.4.89	443	nfC6iCvpK0CUELb0.0.0	msedge.exe
06.12.2023 15:45:34	Closed	TCP	sb.scorecardresearch.com	6.6.4.252	443	Y3YFX0LR+0qtvXSj.0.0	msedge.exe

Questions?

Thank you!